UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Technical Conference) Docket No. AD17-8-000
)
)

STATEMENT OF NATHAN MITCHELL
ON BEHALF OF THE
AMERICAN PUBLIC POWER ASSOCIATION

PANEL IV: GRID SECURITY

I. INTRODUCTION AND SUMMARY

The American Public Power Association ("APPA") submits these comments in the above-referenced proceeding for Nathan Mitchell, APPA's Senior Director of Electric Reliability Standards and Security.

1. APPA and its member utilities have supported the efforts of the industry led Critical Infrastructure Protection (CIP) standard drafting teams to develop risk-based standards through the North American Electric Reliability Corporation (NERC) standard development process. APPA believes that the CIP standards need to reach a steady state and is encouraged by the Commission's staff recently soliciting input from industry on how the standards can be made more efficient while maintaining their effectiveness.

2. APPA agrees that more can and should be done to address the cyber risks to electric utilities, but these efforts should be focused on voluntary programs being developed beyond the NERC standard development process.

3. APPA has partnered with the U.S. Department of Energy (DOE), and has signed Cooperative Agreement, to undertake an extensive multi-year, multi-task project of improving the cyber resiliency and security posture of public power utilities. The project goal is to improve the resiliency and cybersecurity infrastructure within public power utilities. Some of the project's key areas of focus are listed here, and detailed descriptions are given in the comment section:

    a. Conduct Baseline Assessments
    b. Evaluate Information Sharing Tools and Technologies
    c. Develop Targeted Training Opportunities
    d. Conduct Technical Workshops, Exercises, and/or Roundtable Discussions
    e. Develop a Cyber Resiliency and Security Roadmap (Roadmap)
    f. Investigate Cybersecurity Workforce Development Opportunities
    g. Develop an Incident Response Model Playbook (Playbook)

II. DESCRIPTION OF APPA

APPA is the national service organization representing the interests of the nation's 2,000 not-for-profit, community-owned electric utilities. Public power utilities are in every state except Hawaii. They collectively serve over 49 million people and account for 15 percent of all sales of electric energy (kilowatt-hours) to ultimate customers. Public power utilities are load-serving entities, with the primary goal of providing the communities they serve with safe, reliable electric service at the lowest reasonable cost, consistent with good environmental stewardship. This orientation aligns the interests of the utilities with the long-term interests of the residents and businesses in their communities. Approximately 250 public power utilities are NERC Registered entities who have requirements to comply with the NERC Critical Infrastructure Protection (CIP) standards. Accordingly, APPA has a vital interest in developing workable cyber security standards for NERC registered entities, along with encouraging voluntary cyber security programs for the rest of the public power community.

III. COMMENTS:

In the Reliability Technical Conference Agenda, the Commission posed the following questions to Panel IV:

> Cybersecurity continues to be a rapidly evolving risk to the Bulk-Power System. CIP Reliability Standards are designed to mitigate the cybersecurity risks to bulk electric system facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cybersecurity incident, would affect the reliable operation of the Bulk-Power System. The 2015 and 2016 cyber-attacks on the electric grid in Ukraine are examples of how cyber systems used to operate and maintain interconnected networks, unless adequately protected, may be vulnerable to cyber-attack.
>
> a. While controls in the CIP Reliability Standards reduce the risk of cyber-attacks, additional controls or modifications may further mitigate potential

impacts on the operation of the Bulk-Power System. Which controls have been most effective? Are there additional controls, modifications, or voluntary actions that should be considered to improve cybersecurity? What partnerships should the Commission form or strengthen to help improve the overall cybersecurity posture of the Bulk-Power System?

b. A system is only as secure as the people who run and operate it. What can the Commission do to facilitate or encourage a strong cyber workforce?

APPA and its member utilities have supported the efforts of the industry led CIP standard drafting teams to develop risk-based standards through the NERC standard development process. APPA believes that the CIP standards need to reach a steady state and is encouraged by the Commission's staff recently soliciting input from industry on how the standards can be made more efficient while maintaining their effectiveness. Finalizing the standard drafting process for NERC CIP standards will help registered entities focus on the security of their system rather than modifying existing compliance structures to address a continuous standard revision process. The industry has spent many years in the development of the current versions of the NERC CIP standards to address the Commission's previous directives. The time has come to allow utilities to focus their limited resources on implementing security controls to address cyber risks rather than compliance risks. A full cycle of audits on the existing standards should be completed prior to revising the CIP standards again. If the Commission finds it necessary to modify the CIP standards, any directive should be cost-effective and risk- and performance-based.

APPA agrees that more can and should be done to address the cyber risks to electric utilities, but these efforts should be focused on encouraging use of voluntary programs being developed beyond the NERC standard development process. APPA would like to highlight one voluntary program being developed to help public power utilities address cyber risk. As we provide the description of this effort we believe the Commission will recognize how it meshes with other industry, laboratory, and university cyber security efforts.

APPA and DOE Cooperative Agreement

APPA has evaluated its members and concluded that many mid-to-small sized public power utilities outside of the NERC Registry have unique organizational structures including systems control and monitoring, internal or city information technology departments, varied leadership/governance models, and use of third party service providers. Because of the multi-layer structure of these organizations a program was needed to help public power utilities improve recognition of threats and their possible escalation. The initial evaluation showed that public power utilities want additional education, coordination, capability building, and pre-established resources to monitor and detect threats, maintain situational awareness among decision makers, and respond properly to threats and indicators of varying degrees.

APPA has partnered with DOE, and has signed a Cooperative Agreement, to undertake an extensive multi-year, multi-task project of improving the cyber resiliency and security posture of public power utilities. The project goal is to improve the resiliency and cyber security infrastructure within public power utilities. In this project, APPA will accelerate its efforts to help public power utilities to better understand and implement resiliency, cybersecurity and cyber-physical solutions, including refining and improving the adoption of advanced control concepts, where applicable, to achieve security infrastructure improvements.

With this program APPA is providing public power utilities with an array of security tools, technologies, and programs so that the community is better able to understand, install, and implement new cyber and physical resiliency and security systems. Importantly, this program will bolster the cyber security protection for many small utilities that are not part of the Bulk Electric System and thereby not registered with NERC.

Over the project performance period, APPA will undertake the following tasks: 1) conduct and support cyber resiliency and security assessments; 2) conduct, and evaluate on-site vulnerability assessments; 3) research, evaluate, deploy, and integrate both commercial and pre-commercial security technologies; and 4) research, evaluate, and implement information sharing mechanisms.

The purpose of completing these tasks is to deploy cyber and physical security technologies, develop tools, write and disseminate educational resources, update guides, conduct training sessions, share research findings and undertake outreach efforts to assist public power utilities improve their security infrastructure.

Some of the project's key tasks are detailed below:

Conduct Baseline Assessments:

The public power baseline assessment is critical for development of a public power security framework. The baseline assessment includes data on security and resilience capabilities, risk, and/or demographics of public power utilities. The demographic analysis led to the creation of criteria for establishing what is a "small," "medium," and "large" public power utility. APPA used the DOE Electricity Sector Cybersecurity Capabilities Maturity Model (ES-C2M2) tool to obtain input from a sample of public power utilities to develop a baseline of existing cyber resiliency and security capabilities and better define the current resiliency landscape in public power.

Based on the results of the demographic analysis and baseline assessment, APPA developed a tailored cybersecurity maturity model for small and medium sized public power utilities. The model utilizes relevant NERC standards, the NIST Cybersecurity Framework, and DOE ES-C2M2.

The maturity model was determined to be a useful tool for public power utilities to understand the characteristics of mature cyber security programs, processes, and tools. The maturity model will help public power utilities to enhance their cybersecurity programs based on their organizational structure and risk profile.

APPA utilized a contractor to conduct onsite vulnerability assessments at several utilities. These assessments utilized the ES-C2M2, network mapping technologies along with a physical security assessment. Onsite assessments were the most thorough protocol to determine security maturity. The assessments are intended to identify security capabilities and needs of public power utilities.

Evaluate Information Sharing Tools and Technologies

Public power utilities are encouraged to sign up for the E-ISAC as the preferred source of threat information of the electricity industry. APPA has begun to evaluate information sharing tools and technologies that will improve threat information sharing between public power utilities and the E-ISAC. These information-sharing methodologies will incorporate a variety of technologies to reduce the time burden placed on the reporting entities, while ensuring interconnectivity with public and private partners in public safety, security, and community resiliency. APPA wants to evaluate secure information sharing platforms that best serve public power utilities. A risk-based framework is being explored for determining priority levels for the dissemination of secure messages and notifications. Recommendations will be developed and submitted to the E-ISAC on how best to categorize, assess, disclose, and disseminate secure threat information that is useful and usable for public power utilities.

Develop Targeted Training Opportunities

Training is essential to ensuring the public power workforce understands and uses the training tools to further enhance their cybersecurity maturity level. APPA members were surveyed and a majority of respondents requested more training and other guidance to help develop or enhance their cyber security program. Each year APPA provides several conferences and standalone training opportunities for its members and they rely on these sessions to provide low cost opportunities to educate their employees. Cyber security training will be incorporated into these sessions using project funding to reduce the cost.

APPA will test the training materials used at facilitated Association training sessions to receive input on the usefulness to public power utilities of various education formats. The course agendas, instructors and educational materials used will be evaluated to determine the most effective and efficient direction for future training for public power utilities. Investigation will take place on the feasibility of an online, on-demand training platform to support ongoing cybersecurity training.

Conduct Technical Workshops, Exercises, and/or Roundtable Discussions

APPA facilitated technical workshops, exercises and/or roundtable discussions to challenge assumptions and test out models developed in this Project. 14 tabletop exercises were conducted the attendees found the discussion very valuable and requested more sessions at regional meetings. APPA will continue to conduct tabletop exercises and other workshops. The purpose of continued exercises is to reach a wide audience and perspectives to gather additional insight into the cybersecurity needs unique to public power utilities. APPA will also evaluate the effectiveness of a "tabletop exercise in a box" tool.

Develop a Cyber Resiliency and Security Roadmap (Roadmap)

APPA plans to develop and pilot a Public Power Cyber Resiliency and Security Roadmap (Roadmap) that will outline the strategic and tactical steps needed for public power utilities to harden their systems to achieve cyber resiliency and security infrastructure improvements. The Roadmap may include, but not be limited to, policies and procedures templates, incident response case studies, a cyber asset tracker methodology, a procurement guide, and metrics on how to track progress toward improving cyber and physical maturity.

Investigate Cybersecurity Workforce Development Opportunities

Public power utilities often face difficulties in identifying and recruiting qualified cyber and physical security local candidates due to their location and/or size. Working with universities, community colleges and other educational and training institutions across the nation, APPA will explore the development of opportunities and/or programs that meet the staffing needs of public power utilities and that may provide for shared resources and training. The purpose of this task is to enhance the security workforce within public power communities and provide opportunities for college students to intern at public power utilities in the cybersecurity field (and eventually become employed in this sector). An advisory group will be established to undertake research on which educational institutions provide programs that address public power cybersecurity staffing needs. APPA will evaluate the educational programs identified and determine if online opportunities can be developed so that cybersecurity educational programs can be shared among public power utilities in a specific region.

Identifying workforce candidates continues to be a challenge facing public power utilities due to their size and location. Providing educational and internship opportunities to potential full time employees will result in a security trained public power workforce.

Develop an Incident Response Model Playbook (Playbook)

Based on findings that a more focused incident response plan is needed at most public power utilities, APPA will develop a model Playbook which will address potential roles and responsibilities within a small public power utility in the case of a security incident. In many small utilities, one person has many roles and responsibilities. As such, a step-by-step Playbook on what actions to take first, who to coordinate with, and other types of response activities will supplement current mutual aid programs. The Playbook may include scenarios, among other useful tools. Exercises will be held to demonstrate the usefulness of the Playbook and to receive feedback on ease of use and applicability. The Playbook will be coordinated with other industry incident response playbooks such as the one created for the Electricity Sector Coordinating Council (ESCC.)

Conclusion:

APPA believes this and other voluntary cyber security programs will help improve the overall cyber security posture of the Bulk-Power System.

We appreciate the opportunity to provide these written comments for the record.